Departamento de informática

TRABAJO FIN DE GRADO

CURSO DE SEGURIDAD INFORMÁTICA MEDIANTE PODCASTS

Autor: Gala Bernal García

Tutor: Lorena González Manzano

Leganés, Septiembre de 2014

Agradecimientos

En primer lugar me gustaría agradecer a mi familia el apoyo que me han dado día tras día desde que comenzó este nuevo reto, porque gracias a ellos he conseguido llegar a ser lo que soy.

A Nano, por todo y por mucho más.

A mi tutora por la ayuda que me ha proporcionado y por no tirar la toalla en este largo recorrido que hemos vivido juntas.

Y por último quiero agradecer a Alberto García y Francisco Valera de Ingeniería Telemática la plantilla inicial, que ha sido adaptada a este proyecto.

Resumen

Actualmente existen numerosos cursos sobre criptografía en la web. Pero muchos de ellos están basados en artículos, diapositivas u otro tipo de documentación.
Son muy pocos los cursos que están basados en podcasts y la gran mayoría de estos se basan en entrevistas.

La idea principal de la realización de este proyecto surge tras hallar diversas dificultades a la hora de encontrar cursos de aprendizaje orientados a estudiantes con deficiencias visuales.

La idea de que sea un curso sobre criptografía surge porque actualmente el objetivo de la criptografía continua siendo proporcionar comunicaciones seguras sobre canales inseguros. Por este motivo es importante que los usuarios tengan unos conocimientos básicos sobre ella, ya que actualmente es un tema de una gran relevancia.

La importancia de la criptografía [18] reside en que es el único método actual capaz de hacer cumplir el objetivo de la Seguridad Informática, mantener la confidencialidad, integridad y autenticidad de un mensaje enviado. Además de ser la herramienta principal para el desarrollo y estabilidad del comercio electrónico, también está al alcance de todos. por lo tanto todo el público debe tener acceso a dicha información, conocer qué es, sus tipos y las diferentes aplicaciones que se le da actualmente.

Con el desarrollo de este proyecto se consigue ofrecer, acercar y facilitar un curso sobre criptografía orientado principalmente a usuarios con algún tipo de deficiencia visual.

Además con este curso se pretende llegar al mayor público posible., ya que la utilización de podcasts favorece este hecho. La información escuchada es más atractiva, amena y divertida para el resto de usuarios del curso, a pesar de que los usuarios

principales tienen alguna deficiencia visual. Además la web se ha desarrollado en dos idiomas incluido los podcasts, con el fin de poder conseguir y favorecer este objetivo.

Por último este curso busca que los usuarios aprendan que es la criptografía, su historia, los diferentes tipos que hay y las distintas aplicaciones que se le da actualmente. Para que los usuarios puedan comprobar que es lo que han aprendido en cada episodio se proporciona un autoevaluable para que puedan medirlo. De esta manera los usuarios pueden probar cuales son los conocimientos que han adquirido tras escuchar cada podcasts.

Abstract

Nowadays there are many courses on cryptography on the web. But many of them are based on papers, slides or other documentation.
A few courses are focused on podcasts and most of them are based on interviews.
This project has been developed due to it seems to be very difficult to find training courses aimed at student with visual impairments.

The idea of the course on cryptography arises because the objective of the cryptography is to provide secure communications over insecure channels. Therefore it is important that users have a basic understanding of it, since it is currently a topic of great relevance.

The importance of cryptography [18] is that it is the only current method able to enforce the objective of Computer Security, to maintain confidentiality, integrity and authenticity of a message sent. It is also the main tool for the development and stability of e-commerce, it is also available to everyone. For this reason all the public should have access to that information, to know what are the different types and applications that are currently given.

With the development of this project a course on cryptography mainly aimed at users with some kind of visual impairment is provided.

This course tries to reach the largest possible audience, since the use of podcasts helps this fact. The information is heard attractively, enjoyable and pleasantly by other users of the course, even though the main users have some visual impairment. Also the web and the podcasts have been developed in two languages, in order to achieve and support this objective.

Finally, this course seeks users to learn what cryptography is, what its history is, and what the different types and the different applications that are currently given are. To

allow users to check what they have learned in each episode a self-assessable is provided so they can measure it. Thus users can know which the knowledge that they get after hearing each podcasts is.

Índice general

Índice de tablas

CAPÍTULO 3

CAPÍTULO 5

CAPÍTULO 6

Índice de figuras

CAPITULO 3

CAPÍTULO 4

CAPÍTULO 5

Capítulo 1

Introducción y objetivos

1.1 Introducción

En el año 500 a.C. los griegos fueron los primeros en tener la necesidad de utilizar la criptografía, con el fin de ocultar información. . Para ello utilizaban un cilindro en el cual se enrollaba una tira de cuero, este objeto era y es conocido como “scytale”. Durante el transcurso de los años han sido muchos los que han ido teniendo la necesidad de utilizar la criptografía con el fin de poder ocultar o enmascarar la información para que ningún usuario no autorizado pudiera conocer dicha información.

Actualmente, el objetivo de la criptografía continua siendo proporcionar comunicaciones seguras sobre canales inseguros. Por este motivo es importante ser consciente de las diferentes amenazas a las que nos exponemos al utilizar e intercambiar información en formato electrónico.

La importancia de la criptografía [18] reside en que es el único método actual capaz de hacer cumplir el objetivo de la Seguridad Informática, mantener la confidencialidad, integridad y autenticidad de un mensaje enviado. Además es ser la herramienta principal para el desarrollo y estabilidad del comercio electrónico. Además es una herramienta que

está al alcance de todos, por este motivo todo el público debe tener acceso a conocer qué es, sus tipos y las diferentes aplicaciones que se le da actualmente.

Este curso ofrece al público general el acceso a información sobre este tema de una manera diferente a lo habitual, debido a que está basado en podcasts. Además con los podcasts se facilita el acceso a esta información a los usuarios con algún tipo de deficiencias visuales, ya que a través de los podcasts se les facilita el aprendizaje a este tipo de usuarios.

Un podcast [19] es un archivo de audio digital, al que puedes acceder de forma automática. El contenido puede ser de lo más diverso: programas de conversación, música, sonidos ambientales, etc. Generalmente los podcasts son gratuitos y de libre acceso. Cualquier persona, desde cualquier lugar del mundo puede suscribirse, bajar o reproducir el contenido del audio a través de un podcast.

1.2 Motivación

La idea principal de la realización de este proyecto surge tras hallar diversas dificultades a la hora de encontrar cursos de aprendizaje orientados a estudiantes con deficiencias visuales, es decir, discapacidades visuales sobre temas concretos de seguridad informática. Es posible encontrar información y cursos asociados a la criptografía pero ninguno de ellos se enfoca a un público con deficiencias visuales.

Otro problema encontrado es la gran cantidad de contenidos que se encuentran en la web sin disponer de una fuente de referencia que garantice la calidad de los mismos. Internet es utilizado día tras día por multitud de usuarios y por ello los contenidos presentados han de tener una calidad y fiabilidad adecuada.

Por último, otro problema es que la información disponible no siempre es accesible a todos los públicos, bien por su complejidad o bien por su presentación. Por ejemplo, las personas con deficiencias visuales han de tener contenidos adaptados que se adecúen a ellos, siendo los podcasts una posible solución a este problema,

Por estos motivos surgió la idea de crear un curso sobre criptografía. Este curso presenta unos contenidos contrastados y adaptados a personas con deficiencias visuales, es decir, fáciles tanto de entender como de asimilar, por ejemplo, evitándose la descripción de matemáticas complejas que serían inapropiadas para una lección en formato audio.

1.3 Objetivos

El objetivo fundamental de este proyecto es ofrecer, acercar y facilitar un curso sobre criptografía orientado principalmente a usuarios con algún tipo de deficiencia visual. Por este motivo se han elegido los podcasts como formato para exponer la información. De esta manera estos usuarios podrán escuchar y aprender sin necesidad de leer la información.

El segundo objetivo principal de este curso es llegar al mayor público posible. Por este motivo la utilización de los podcasts favorece a este hecho. La información escuchada es más atractiva, amena y divertida para el resto de usuarios del curso, a pesar de que los usuarios principales tienen alguna deficiencia visual. Además la web se ha desarrollado en dos idiomas incluido los podcasts, con el fin de poder llegar a un mayor número de usuarios.

El último objetivo de este curso es que todos los usuarios aprendan que es la criptografía, su historia, los diferentes tipos que hay y las distintas aplicaciones que se le da actualmente. Para que los usuarios puedan comprobar que es lo que han aprendido en cada episodio se proporciona un autoevaluable para que puedan medirlo. De esta manera los usuarios pueden probar cuales son los conocimientos que han adquirido tras escuchar cada podcasts.

1.4 Fases del proyecto

Este apartado expone los distintos pasos que se han seguido para llevar a cabo este proyecto. Los pasos seguidos son los siguientes:

- **Paso 1:** En primer lugar se realizó un estudio previo de los distintos cursos online sobre seguridad criptográfica basados en podcast disponibles actualmente..

- **Paso 2:** En segundo lugar se comenzó la búsqueda de información para poder construir el contenido de cada uno de los episodios que forman el curso. Para obtener toda la información se realizó un estudio de las diferentes fuentes de información o referencias y además se contrastó la información con libros, artículos, apuntes de diferentes asignaturas de la carrera y con profesores expertos en la materia.

- **Paso 3:** En tercer lugar se estructuró el contenido del curso en un número de episodios y se comenzó la redacción de cada uno de ellos basándose en la información obtenida en el paso dos.

- **Paso 4:** Luego el siguiente paso que se realizó fue la grabación de los podcast primero en castellano y tras su traducción, estos fueron grabados en inglés.

- **Paso 5:** En quinto lugar se comenzó el diseño y posterior desarrollo del sitio web. Este sitio web es utilizado para colgar los distintos podcast. Además, por cada episodio se ha realizado un podcast y un autoevaluable para que los usuarios puedan comprobar que han aprendido en cada episodio.

- **Paso 6:** En penúltimo lugar se realizaron una batería de pruebas para comprobar que todo funcionaba de manera correcta.

- **Paso 7:** Por último lugar se subió el sitio web construido para que esté disponible para los usuarios.

1.5 Recursos empleados

Este proyecto consiste en el desarrollo de un curso de criptografía y de una página web en la que colgarlo y dejarlo accesible a los usuarios. En la realización de este proyecto ha sido necesaria la utilización de muchos recursos.
Para poder explicar los diferentes recursos que se han empleado en la elaboración del proyecto se van a diferenciar en software y hardware.

En primer lugar se hablará de los recursos software usados en la implementación del proyecto, estos son:

Word 2010 [1]
Software que capaz de crear documentos. Puede usarse para crear documentos utilizando fotografías, imágenes o fondos multicolores e incluso tablas. También proporciona varias características de ayuda para la creación de texto con el fin de poder crear documentos profesionales.

Audacity [2]
Editor de audio libre. Este software es fácil de usar y además multipista para diferentes sistemas operativos como Windows, Mac OS X, GNU/Linux entre otros. Audacity puede utilizarse para:

- Grabar audio en vivo.
- Grabar el sonio que se esté escuchando en el equipo, solo si se tiene un sistema operativo Windows Vista o superior.
- Editar archivos de audio en diferentes extensiones.
- Convertir cintas y grabaciones a sonio digital.

- Cortar, mezclar, copiar, unir sonidos.
- Etc.

Notepad++ [3]
Software que permite crear y editar código fuente siendo capaz de soportar diferentes lenguajes. Es el sucesor del Bloc de notas debido a que mejora y amplía su funcionalidad.

Yuml [20]
Servicio web que permite crear diagramas UML de manera sencilla y sin requerir ninguna descarga.

Free FTP [21]
Programa FTP gratuito, diseñado para ser potente y fácil de usar. Permite conectarse a su servidor con el clic de un botón. Este programa es capaz de manejar todas las variaciones de FTP que hay, es decir, se puede elegir entre FTP, SFTP, FTPS y sus diferentes métodos de encriptación. Incluso puede manejar HTTP.

GanttProject [10]
Software gratuito usado para la administración de proyecto utilizando diagramas de Gantt. Algunas de sus características son:

- Diagramas de Gantt.
- Diagramas de PERT.
- Admite importar documentos de MS Project.
- Reportes en PDF y HTML.

En segundo lugar se describen los medios hardware utilizados durante la realización de este proyecto:

Auriculares [15], aparato que consta de dos piezas unidas por una tira normalmente curva y ajustable a la cabeza. Estos se acoplan a los oídos para la recepción del sonido.

Micrófono [15], aparato utilizado para convertir las ondas sonoras en energía eléctrica y viceversa en métodos de grabación y reproducción de sonido. Esta conversión consiste fundamentalmente en un diafragma atraído interrumpidamente por un electroimán, que, al vibrar, varía la corriente transmitida debido a las diferentes presiones a un circuito.

Estudio de grabación [16], lugar destinado al registro de voz y música, en condiciones tales que al reproducir posteriormente el material obtenido.

1.6 Estructura de la memoria

En este apartado se explicará brevemente que contenido se va a tratar en cada sección.

- **Capítulo 1:** Se da una visión general del proyecto, incluyendo la motivación y los objetivos que han llevado a la realización del mismo.

- **Capítulo 2:** Se realiza un planteamiento del problema, en este capítulo se analiza el estado del arte, donde se muestra la búsqueda previa a la realización del proyecto, en la cual se buscaron aplicaciones similares, que puedan satisfacer necesidades parecidas, y diferentes herramientas para poder desarrollar este prototipo. A continuación se explica el alcance del proyecto y las herramientas que han sido empleadas finalmente.

- **Capítulo 3:** Se describen las características principales del proyecto centralizándose en los requisitos software. Se comienza con una separación entre requisitos funcionales y no funcionales. Luego se describe el plan de pruebas de aceptación que se ha realizado para validar el sistema. Por último se muestran las matrices de trazabilidad.

- **Capítulo 4:** Se muestra el diseño que se ha realizado para la web, se exponen los elementos que forman el sistema.

- **Capítulo 5:** Se muestra el modelo del ciclo de vida, la planificación que se ha seguido en el proyecto y además se estudia la desviación que ha sufrido la planificación inicial frente a la real.

- **Capítulo 6:** Se muestra el presupuesto del proyecto y además se realiza un análisis de gastos detallados. .

- **Capítulo 7:** Se describen las conclusiones obtenidas tras el desarrollo del proyecto.

- **Capítulo 8:** Se describen posibles trabajos futuros a partir de lo realizado en este proyecto.

Capítulo 2

Estado del arte

2.1 Análisis del estado del arte

En esta sección se ofrece un análisis sobre las diferentes propuestas que existen sobre cursos de criptografía.

Actualmente existe una amplia variedad de cursos sobre criptografía. Los cursos [12] [13] pueden estar compuestos por podcasts, transparencias, artículos o incluso vídeos sobre dichos temas, pero la mayoría son transparencias y artículos. En este caso nos centraremos en analizar cursos de criptografía compuestos por podcasts ya que como se ha mencionado anteriormente en el capítulo 1, el público objetivo principalmente son personas con deficiencias visuales. Estos cursos están orientados a personas o usuarios sin conocimientos en el tema, pues otro de los objetivos es conseguir que estos adquieran unos conocimientos sobre el tema obteniendo una visión general. Todos los cursos encontrados se analizan a continuación:
Dado que el objetivo es proporcionar un curso para el mayor número de usuarios posibles, se analizarán los podcast que estén tant en español como en inglés.

En primer lugar se analiza un podcast encontrado en la web JavaHispano [4][], en el cual se habla de Criptografía y Firma Digital. Este podcast se caracteriza por ser una

entrevista de una emisora de radio a dos investigadores de la Universidad Jaume I, concretamente Ricardo Borillo y Paúl Santapau. Este podcast se divide en dos partes:

- En la primera parte se tratan conceptos teóricos sobre criptografía y firma digital, concretamente sobre algoritmos, técnicas y un poco de legislación de la administración pública.
- En la segunda parte se habla sobre seguridad informática, se dan una serie de conceptos básicos sobre este tema, pero sobre todo se centra en el CryptoApplet, debido a que los dos entrevistados son los responsables de este proyecto.

En segundo lugar se analizará un podcast disponible en la web crimenDigital [5], que tiene por nombre "Criptografía vs Análisis Forense". Este podcast también se caracteriza por ser una entrevista de una emisora de radio, en este caso al Dr. Roberto Gómez, en la cual hablan sobre las diferencias entre la criptografía y el análisis forense, es decir pros y contras de cada uno.

En tercer lugar se analizará un podcast disponible en la web ivoox [6], que tiene el nombre de "El elixir de la confianza. Criptografía". Este podcast está publicado en el Podcast de "Ulises y la Ciencia" en Ciencia y naturaleza. A pesar de estar orientado a la criptografía, en su comienzo se habla de la desconfianza crece por doquier afectando a la mayor parte de los aspectos de la vida, como por ejemplo: los bancos, los gobiernos, los políticos, etc. Es el único podcast que no es una entrevista de una emisora de radio, sino un conjunto de reflexiones que finalmente son orientadas a la criptografía.

En cuarto lugar se analizará un podcast disponible en la web de ivoox [4], aunque pertenece a un programa llamado Eureka [14]. Este podcasts tiene por nombre "La criptografía: mensajes ocultos.". En este podcasts se habla sobre mensajes ocultos, como se cifran y como se descifran. Se habla sobre algunas técnicas criptográficas que se utilizan para hacernos ocultos a los ojos de los demás y la cantidad de operaciones matemáticas complejas que están detrás de la criptografía. Este podcasts al igual que los primeros que se han analizados es una entrevista a una investigadora de la universidad Pompeu Fabra [17], Vanesa Daza.

En conclusión la gran mayoría de los podcast encontrados en la web son entrevistas realizadas por una emisora de radio sobre partes de la criptografía. Estos podcast son interesantes ya que los entrevistados son personas con grandes conocimientos en la materia, pero también tienen una gran desventaja, ya que estos podcast cuentan varias cuestiones sobre criptografía pero no proporcionan un curso, aunque básico pero con cierta completitud. Además estos podcasts contienen publicidad y eso puede ser perjudicial ya que puede desconcentrar al usuario perdiendo el hilo del tema.

Por otro lado se han analizado varios podcasts encontrados en la web en inglés. La cantidad de podcasts encontrados en este idioma son más numerosos, a continuación se analizarán algunos de ellos.

Se comienza analizando algunos de los podcasts encontrados en la web threatpost [5]. En primer lugar se analiza un podcast cuyo nombre es "*Cryptocat Encrypted Chat Vulnerable to Simple Brute Force Decryption*". En él se habla sobre la aplicación Cryptocat, chat basado en cifrado web de código abierto, ya que está teniendo numerosas críticas después de descubrir algunas vulnerabilidades que ponían en riesgo los chats.

En segundo lugar se analiza otro podcast que tiene por nombre "Crypto Gains Ramp Up Calls to Get Ahead of Inevitable RSA Algorithm Downfall". En este podcasts se habla sobre los avances criptográficos que se han acelerado en los últimos meses en áreas como el cálculo de logaritmos discretos. Los expertos creen que estos avances pueden llevar a la ruptura del algoritmo RSA en un futuro no muy lejano.

En tercer lugar se analiza otro podcast que tiene por nombre "Exploits Weakness in RC4 Cipher to Decrypt User Sessions". En él se habla sobre el cifrado de flujo RC4 y de todo el tiempo que lleva siendo utilizado. Se habla sobre la debilidad de RC4 que podría permitir a un atacante descifrar el flujo de claves. Además ahora un criptógrafo ha publicado un ataque que aprovecha dicha vulnerabilidad y causa serios problemas con las implementaciones TLS.

En cuarto lugar se analiza otro podcasts cuyo nombre es "Cryptographers Aim to Find New Password Hashing Algorithm". Este podcast trata sobre la importancia de las claves, ya que estas son las lleves de nuestras identidades en la red y debido a esto son el objetivo principal de los atacantes. En los últimos años ha habido abundantes incumplimientos en los que las contraseñas sin cifrar se han sustraído de las bases de datos y filtrado en Internet. Para solucionar esto un grupo de criptógrafos patrocina un curso para llegar a un nuevo algoritmo hash de la contraseña para mejorar la técnica, ya que presenta algunas vulnerabilidades.

Además se ha analizado un podcast disponible en la web avclub [6]. Este tiene por nombre "Codes! Allied Cryptography in World War II", en él se habla de los códigos y criptogramas utilizados en la Segunda Guerra Mundial. Se aprenderán cosas sobre la máquina enigma, Alan Turing y codificaciones, entre otras cosas.

Otro de los podcasts que se han analizado es el disponible en la web scientificamerican [7], cuyo nombre es "*Quantum Cryptography Comes to Smart Phones*". En este podcast se habla sobre una técnica de cifrado cuántico realizado fuera del Laboratorio Nacional de Los Alamos que podría proporcionar más seguridad a los teléfonos inteligentes, ya que estos tienen muy poca seguridad. Esto es un problema real ya que hay mucha gente que utiliza el móvil como si fuera un ordenador, es decir, para la banca en línea, compras, etc.

La diferencia principal que existe entre los podcast en español y los podcast en inglés es que los ingleses no son entrevistas realizadas por una emisora de radio si no que son ensayos o artículos de investigación leídos. Sin embargo, con independencia del idioma, no existe ningún curso de criptografía basado en podcast.

2.2 Estructura de los episodios

Estas son los distintos episodios que formarán parte del curso sobre criptografía.

1. **Criptografía (PODCAST)**
   1.1.¿Qué es la criptografía?
   1.2.¿Qué tipos de criptografía existen?
   1.3.Aplicaciones de la criptografía en la actualidad.
   1.4.Resumen

2. **Criptografía Clásica (PODCAST)**
   2.1 ¿Cómo surgió la criptografía clásica?
   2.2 Tipos de criptografía clásica.
      2.2.1 Cifrado por Transposición
      2.2.2 Cifrado por Sustitución
   2.3 Resumen

3. **Criptografía Simétrica (PODCAST)**
   3.1 ¿Qué es la criptografía simétrica?
   3.2 ¿Cuáles son las ventajas y desventajas de los algoritmos simétricos?
   3.3 ¿Cómo funciona el cifrado por bloque?
   3.4 Tipos de algoritmos de cifrado por bloque
   3.5 Resumen

4. **Criptografía Asimétrica (PODCAST)**
   4.1 ¿Qué es la criptografía asimétrica?
   4.2 ¿Cómo funciona la criptografía asimétrica?
   4.3 ¿Cuáles son las ventajas e inconvenientes?
   4.4 Algoritmos usados en la criptografía asimétrica
   4.5 ¿Cuáles son las aplicaciones de la criptografía asimétrica?
   4.6 Resumen

5. **Certificados electrónico (PODCAST)**
   5.1 ¿Qué es un certificado electrónico?
   5.2 ¿Cuáles son los usos que se le pueden dar a un certificado electrónico?
   5.3 ¿Cuáles son las entidades públicas emisoras de certificados en España?
   5.4 ¿Cuáles son los certificados del DNI Electrónico?
   5.5 ¿Cuál es la certificación otorgada por la fábrica de moneda y timbre?
   5.6 ¿Cuáles son las ventajas e inconvenientes de un certificado electrónico o digital?
   5.7 Resumen

6. **Firma digital (PODCAST)**
   6.1 ¿Qué es la firma digital?
   6.2 ¿Cómo funciona la firma digital?
   6.3 Propiedades de la firma digital
   6.4 Protocolos usados en la firma digital
   6.5 ¿Cuáles son las ventajas e inconvenientes de la firma digital?
   6.6 ¿Cuáles son las aplicaciones que le da a la firma digital?
   6.7 Resumen

2.3 Alcance del sistema a desarrollar

El prototipo que se ha desarrollado en este proyecto tiene como objetivo principal realizar un curso sobre criptografía con el fin de ayudar a cualquier usuario, con deficiencias visuales.

Los ejemplos de uso que se plantean tienen como objetivo principal realizar un desarrollo utilizando tecnologías existentes. Los motivos por los cuales se ha realizado este proyecto son:

- Facilitar la búsqueda y el aprendizaje a los usuarios con deficiencias visuales.
- Representar la información de una manera más cómoda para poder ayudar a los principales usuarios. Pero también hacerla más atractiva, amena y divertida para el resto de usuarios.
- Como este curso va dirigido a la mayor cantidad de usuarios posibles, por esa razón se ha realizado este curso en dos idiomas, castellano e inglés.

A continuación se van a explicar las dos fases principales que se han seguido para la realización de este curso online sobre criptografía.

Para la realización de este proyecto primero se diseñó el curso, es decir, se buscó mucha información en diferentes fuentes sobre la criptografía. De esta manera se fue estructurando poco a poco el curso en diferentes episodios. En cada episodio se va hablar de un tema concreto de la criptografía, aunque es importante recargar que los episodios van aumentando en nivel de especificación poco a poco, con el fin de que el usuario poco a poco adquiera conocimientos más avanzados sobre el tema.

Cuando los distintos episodios en los que se ha estructurado el curso se redactaron se tradujeron al inglés para que los usuarios pudieran descargarlos en formato pdf a través de la web en ambos idiomas. Finalmente se procedió a la grabación de estos, primero en castellano y después en inglés.

En segundo lugar, se ha realizado una página web siguiendo la WCAG, una guía para crear sitios web accesibles de la W3C. De esta manera se comprueba la accesibilidad de la web.
Es importante recargar que se ha utilizado una plantilla web gratuita y libre para la realización de la web, pero esta se ha modificado con el fin de que sea más accesible para los usuarios con deficiencias visuales.
Esta página está realizada en HTML5.0 y tiene código javascript para la realización de las comprobaciones que requiere la web.

Los dos prototipos principales que se pueden distinguir en la web que se ha implementado para este curso online sobre criptografía son los siguientes:

- Página principal:
  En esta página contiene un resumen general del contenido del curso. Además de tener diversos enlaces a las páginas específicas de cada uno de los episodios que forman el curso. Por último tiene un icono para cambiar la página de idioma, este se encuentra en la parte superior derecha de la pantalla.

- Página detallada:
  Cada episodio del curso tiene una página en la cual se expone un pequeño resumen del contenido del podcast que contiene. El podcast puede ser reproducido desde esa página y además puede ser descargado en formato pdf. Es importante recordar que también cada una de estas páginas contiene un autoevaluuable, a través del cual los usuarios puede comprobar que han aprendido en el episodio. Finalmente en la parte superior derecha se encuentra un icono con el cual se cambia el idioma de la página.

Capítulo 3

Análisis

3.1 Requisitos

3.1.1 Justificación de la clasificación de requisitos

En este apartado se definen los requisitos o capacidades que necesita un usuario para resolver un problema o conseguir un objetivo determinado. Los requisitos que se van a definir serán los siguientes:

- **Requisitos funcionales:** explicación de los servicios que el sistema debe proporcionar, cómo debe reaccionar a una acción en particular.

- **Requisitos no funcionales:** limitaciones que afectan a los servicios o funciones del sistema.

Para recoger los requisitos se seguirá el modelo que se observa en la tabla 3.1.

Tabla 3.1. "Ejemplo de la tabla de requisitos"

Requisitos Software				
Tipo: Funcional				
Id	**Nombre**	**Descripción**	**Complejidad**	**Prioridad**

A continuación se realizará un análisis más detallado de cada uno de los campos.

- **Identificador:** RF (requisitos funcionales) y RNF (requisitos no funcionales). Mientras que NN se corresponde con el número del requisito.
- **Nombre:** calificativo que se le da al requisito.
- **Descripción:** definición especifica que se da del requisito.
- **Complejidad:** grado de dificultad que se le da al requisito. Este campo puede tener como valores: alta, media o baja.
- **Prioridad:** importancia de implantación cuyos valores pueden ser baja, media o alta.

3.1.2 Requisitos funcionales

Los requisitos funciones que tiene el sistema que se ha desarrollado son los descritos en la tabla 3.2.

Tabla 3.2. "Tabla de requisitos funcionales"

Requisitos Software				
Tipo: Funcional				
Id	**Nombre**	**Descripción**	**Complejidad**	**Prioridad**
RF-01	Navegabilidad	Desde cada una de las páginas se debe poder navegar hacía el resto.	Media	Alta
RF-02	Cambio de idioma	Todas las páginas de la web deben tener un enlace para poder cambiar el idioma de esta.	Baja	Alta
RF-03	Icono de idioma correcto	Todas las páginas de la web deben tener un icono con la bandera de un país distinto al lenguaje en el que está escrito en la página.	Baja	Alta

RF-04	Reproducción de un podcast	Cualquiera de las páginas específicas de un episodio del curso debe tener una interfaz que permita la reproducción de un podcast.	Media	Alta
RF-05	Parar una reproducción	Cualquiera de las páginas específicas de un episodio del curso debe tener una interfaz que permita parar la reproducción de un podcast.	Baja	Alta
RF-06	Reanudar una reproducción	Cualquiera de las páginas específicas de un episodio del curso debe tener una interfaz que permita reanudar la reproducción de un podcast que ha sido parado anteriormente.	Baja	Alta
RF-07	Avanzar en una reproducción	Cualquiera de las páginas específicas de un episodio del curso debe tener una interfaz que permita avanzar en la reproducción de un podcast.	Baja	Media
RF-08	Retroceder en una reproducción	Cualquiera de las páginas específicas de un episodio del curso debe tener una interfaz que permita retroceder en la reproducción de un podcast.	Baja	Media
RF-09	Modificar volumen	Cualquiera de las páginas específicas de un episodio del curso debe tener una interfaz que permita modificar el volumen de una reproducción.	Baja	Baja
RF-10	Descargar un archivo de texto	Cualquiera de las páginas específicas de un episodio debe permitir la descarga de un archivo de texto.	Media	Alta
RF-11	Botón de descarga	Cualquiera de las páginas específicas de un episodio del curso debe contener un botón para descargar el archivo de texto correspondiente con cada episodio del curso,	Baja	Alta

3.1.3 Requisitos no funcionales

Los requisitos no funcionales del sistema son los siguientes:

Tabla 3.3. "Tabla de los requisitos no funcionales del sistema"

Requisitos Software				
Tipo: Funcional				
Id	**Nombre**	**Descripción**	**Complejidad**	**Prioridad**
RNF-01	Tamaño de las imágenes	Las imágenes que tendrá la web tendrán un tamaño máximo de 100 KB.	Baja	Alta
RNF-02	Tamaño de los podcasts	Todos los podcasts albergados en la web no deben tener un tamaño superior a 1MB.	Baja	Alta
RNF-03	Tamaño de los archivos de texto descargables.	Todos los archivos de texto descargables desde la web no deben tener un tamaño superior a 300KB.	Baja	Alta
RNF-04	Accesibilidad web	La web implementada para este curso online sigue los criterios establecidos por el WAI.	Alta	Alta
RNF-05	Compatibilidad con los navegadores	La web debe ser compatible con las últimas versiones de los diferentes navegadores: ▪ Mozilla Firefox 32.0 ▪ Internet Explorer 10 o 11 ▪ Google Chrome 37.0 ▪ Safari 7.0	Media	Alta
RNF-06	Idioma	El idioma del sistema será castellano y English.	Media	Alta
RNF-07	Acceso simultáneo	La web implementada debe soportar el acceso simultáneo de varios usuarios.	Media	Media
RNF-08	Adaptación a Smartphone y Tablets	Todas las páginas web deben adaptarse a distintas resoluciones de pantalla.	Baja	Media
RNF-09	Disponibilidad completa	Todas las páginas web deben estar disponibles a cualquier hora y durante todo el tiempo que este el curso en la web.	Baja	Baja

3.2 Diseño del plan de pruebas de aceptación

Una vez se han definidos las características del sistema que se ha desarrollado a lo largo de este trabajo fin de grafo se va a proceder a realizar el plan de pruebas de aceptación del mismo.

En esta sección se detalla el plan de pruebas de aceptación del sistema en el cual se muestran las distintas pruebas que se ha de superar y los resultados esperados de estas para que se superen todas las pruebas de aceptación.

En la tabla 3.4 se detalla el plan de pruebas definidos según lo definido en la tabla 3.3.

Tabla 3.4. "Ejemplo de la tabla del plan de pruebas de aceptación"

Pruebas de aceptación			
Id	**Elementos probados**	**Entrada**	**Salida**

A continuación se realizará un análisis más detallado de cada uno de los campos.

- **Identificador:** PA (Prueba de Aceptación) y NN se corresponde con el número del requisito.
- **Elementos probados**: identifica los requisitos funcionales que se prueban.
- **Entrada**: muestra la situación deben darse para poder realizar las pruebas.
- **Salida**: muestra la situación que debe darse para poder pasar la prueba.

Tabla 3.5. "Plan de pruebas de aceptación del sistema"

Pruebas de aceptación			
Id	**Elementos probados**	**Entrada**	**Salida**
PA-01	RF-01	Se está navegando en una página de la web y se pincha sobre cualquiera de los enlaces para navegar hacía otra página del sistema.	Se navega correctamente hacía la página seleccionada a través del enlace seleccionado.
PA-02	RF-04	Se está navegando en cualquiera de las páginas	Se debe reproducir el podcast.

		de un episodio se pulsa sobre el icono del play en la interfaz de reproducción que tiene la página.	
PA-03	RF-05	Se está navegando en cualquiera de las páginas de un episodio se pulsa sobre el icono de stop en la interfaz de reproducción que tiene la página.	Se debe para la reproducción del podcast.
PA-04	RF-06, RF-04	Se debe haber parado anteriormente la reproducción de un podcast.	Se debe reanudar la reproducción del podcast.
PA-05	RF-01, RF-02, RF-03	Se debe pinchar sobre el icono de la bandera para cambiar el idioma de la web.	Se debe cambiar el idioma de la página en la que se está navegando.
PA-06	RF-07	Se debe estar reproduciendo alguno de los podcasts del curso. Se debe avanzar sobre la barra de reproducción de este.	Se debe avanzar en la reproducción del podcast.
PA-07	RF-08	Se debe estar reproduciendo alguno de los podcasts del curso. Se debe retroceder sobre la barra de reproducción de este.	Se debe retroceder en la reproducción del podcast.
PA-08	RF-09	Se debe estar reproduciendo alguno de los podcasts del curso. Se debe modificar el volumen del podcast utilizando el icono del volumen de la interfaz.	Se debe modificar el volumen de la reproducción del podcast.
PA-09	RF-10, RF-11	Se debe estar navegando en una de las páginas de los episodios del curso y se debe comprobar que tiene un botón de descarga.	Se debe comprobar que la página tiene un botón para descargar archivos de texto en formato pdf.

PA-10	RF-10	Se debe pinchar sobre el botón de descarga.	Se debe comprobar que se descarga el archivo de texto de ese episodio.

3.3 Casos de uso

En este apartado se definen y explican los diferentes casos de uso del sistema que se ha desarrollado.

Es importante definir antes de comenzar con los casos de usos es que es un caso de uso, descripción de las acciones necesarias para poder ejecutar el proceso.

Para recoger los casos de uso se seguirá el modelo que se observa en la tabla 3.6.

Tabla 3.6"Ejemplo de la tabla de casos de uso"

Id:	
Nombre:	
Autor:	
Descripción:	
Actores:	
Precondiciones:	
Postcondiciones:	
Flujo Normal:	

- **Identificador:** CU identifica un caso de uso y NN identifica al número de este.
- **Nombre:** calificativo que identifica al caso de uso.
- **Autor:** nombre de la persona que ha definido los casos de uso.
- **Descripción:** definición detallada del caso de uso.
- **Precondiciones:** situaciones que deben cumplirse para llevar ejecutar el caso de uso.
- **Post-condiciones:** situaciones que se producen al conseguir el objetivo del caso de uso.
- **Flujo Normal:** listado de acciones que deben llevarse a cabo para conseguir el resultado esperado

Tabla 3.7. "Caso de uso 1"

Id: CU-01	
Nombre:	Navegabilidad entre páginas
Autor:	Gala Bernal García
Descripción: Navegar entre las distintas páginas de la web.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario se encuentra navegando en alguna de las páginas del sistema.	
Postcondiciones: ▪ El usuario se encontrará navegando en otra página distinta del sistema.	
Flujo Normal: 1. El usuario debe pinchar sobre algunos de los enlaces que tienen todas las páginas para navegar al resto de páginas.	

Tabla 3.8. "Caso de uso 2"

Id: CU-02	
Nombre:	Reproducción de un podcast.
Autor:	Gala Bernal García
Descripción: Reproducir cualquiera de los podcasts que se encuentran en las distintas páginas de la web.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario se encuentra navegando en alguna de las páginas del sistema que tiene un podcast.	
Postcondiciones: ▪ El podcast comenzará a reproducirse.	
Flujo Normal: 1. El usuario debe pinchar sobre el icono de play que tiene la interfaz de reproducción del podcast.	

Tabla 3.9. "Caso de uso 3"

Id: CU-03	
Nombre:	Parar reproducción
Autor:	Gala Bernal García
Descripción: Parar la reproducción de un podcast que está siendo reproducido en ese momento.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario debe estar reproducción un podcast de la web.	
Postcondiciones: ▪ La reproducción del podcasts debe pararse.	
Flujo Normal: 1. El usuario debe pinchar sobre el icono de stop que tiene la interfaz de reproducción del podcast.	

Tabla 3.10. "Caso de uso 4"

Id: CU-04	
Nombre:	Reanudar reproducción
Autor:	Gala Bernal García
Descripción: Reanudar la reproducción de un podcast parado anteriormente.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario debe haber parado la reproducción de un podcast de la web.	
Postcondiciones: ▪ La reproducción del podcasts debe reanudarse.	
Flujo Normal: 1. El usuario debe pinchar sobre el icono de play que tiene la interfaz de reproducción del podcast.	

Tabla 3.11. "Caso de uso 5"

Id: CU-05	
Nombre:	Avanzar en la reproducción
Autor:	Gala Bernal García
Descripción: Avanzar en la reproducción de un podcast.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario debe estar reproduciendo o no un podcast.	
Postcondiciones: ▪ La reproducción del podcasts debe avanzar.	
Flujo Normal: 1. El usuario debe deslizar el cursor hacía la derecha sobre la barra de reproducción que tiene la interfaz de reproducción del podcast.	

Tabla 3.12. "Caso de uso 6"

Id: CU-06	
Nombre:	Retroceder en la reproducción
Autor:	Gala Bernal García
Descripción: Retroceder en la reproducción de un podcast.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario debe estar reproduciendo o no un podcast.	
Postcondiciones: ▪ La reproducción del podcasts debe retroceder.	
Flujo Normal: 1. El usuario debe deslizar el cursor sobre la izquierda en la barra de reproducción que tiene la interfaz de reproducción del podcast.	

Tabla 3.13. "Caso de uso 7"

Id: CU-07	
Nombre:	Cambiar idioma
Autor:	Gala Bernal García
Descripción: Cambiar idioma de la web.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario debe estar navegando en alguna de las páginas de la web.	
Postcondiciones: ▪ Toda la web debe de cambiar de idioma.	
Flujo Normal: 1. El usuario debe pinchar sobre el icono de la bandera, situado en la parte superior derecha todas las páginas del sistema.	

Tabla 3.14. "Caso de uso 8"

Id: CU-08	
Nombre:	Modificar volumen
Autor:	Gala Bernal García
Descripción: Modificar el volumen de un podcast	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario debe estar navegando en una página con podcast.	
Postcondiciones: ▪ El volumen del podcast debe modificarse	
Flujo Normal: 1. El usuario debe deslizar el cursor sobre la barra de volumen tiene la interfaz de reproducción del podcast.	

Tabla 3.15. "Caso de uso 9"

Id: CU-09	
Nombre:	Descargar archivo
Autor:	Gala Bernal García
Descripción: Descargar un archivo de texto desde la web.	
Actores: Usuario de la web.	
Precondiciones: ▪ El web está alojada en el servidor. ▪ La web está disponible para utilizarse. ▪ El usuario debe estar navegando en una página con podcast.	
Postcondiciones: ▪ Se descarga un archivo de texto desde la web.	
Flujo Normal: 1. El usuario debe pinchar sobre el botón de descargar un archivo	

A continuación se va a mostrar la descripción grafía de los siete casos de uso que han sido definidos en las tablas 3.7, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14 y 3.15.

Figura 3.1. "Diagrama de los casos de uso del sistema"

3.4 Matrices de trazabilidad

En este apartado se mostrarán varias matrices de trazabilidad entre los distintos tipos de requisitos y los casos de uso.

3.4.1 Requisitos funcionales

Tabla 3.16. "Matriz de trazabilidad de los requisitos funcionales y los casos de uso"

	CU-01	CU-02	CU-03	CU-04	CU-05	CU-06	CU-07	CU-08	CU-09
RF-01	X						X		
RF-02							X		
RF-03	X						X		
RF-04		X							
RF-05			X						
RF-06		X		X					
RF-07					X				
RF-08						X			
RF-09								X	
RF-10									X
RF-11									X

3.4.2 Requisitos no funcionales

Tabla 3.17. "Matriz de trazabilidad de los requisitos no funcionales y los casos de uso"

	CU-01	CU-02	CU-03	CU-04	CU-05	CU-06	CU-07	CU-08	CU-09
RNF-01	X						X		
RNF-02	X	X	X	X	X	X			
RNF-03									X
RNF-04	X						X		
RNF-05	X	X	X	X	X	X	X	X	X
RNF-06							X		
RNF-07	X	X	X				X		X
RNF-08	X	X	X	X	X	X	X	X	X
RNF-09	X	X	X	X	X	X	X	X	X

Capítulo 4

Diseño

4.1 Elementos del diseño arquitectónico

Este proyecto realizado consiste en el desarrollo de un curso de criptografía y de una página web en la que colgarlo y dejarlo accesible a los usuarios.
En este apartado se relatan y explican elementos del diseño arquitectónico de este proyecto, pero antes se van a definir unos conceptos básicos para entender los diferentes elementos que tiene la web implementada

- Podcast [8], archivo de audio que puede ser escuchado y descargado en un ordenador o un dispositivo móvil que pueda reproducir audio, más concretamente archivo de audio con extensión mp4.

- Reproductor multimedia, dispositivo que recopila, organiza y reproduce archivos de audio y video digitales.

- Respuestas ocultas, respuestas que de primeras se encuentran ocultas al usuario. De esta manera el usuario debe seleccionar o pinchar sobre una opción para poder verlas.

- Enlace, texto visualizado en la pantalla que en el código está apuntando a otra dirección URL. Cuando el usuario pulsa sobre este texto la página navega hasta la página de la URL.

- Navegador web [11], software que permite los usuarios rescatar y visualizar documentos de hipertexto, habitualmente implementados en HTML, desde servidores web de todo el mundo a través de la web. Esta red de comunicación y recuperación de información es conocida como WWW.

- Servidor web [9], ordenador remoto que provee los datos solicitados por parte de los navegadores de otras computadoras. Almacenan información en forma de páginas web y por medio del protocolo HTTP lo ceden a petición de los clientes en formato HTML.

- Cuestionario autoevaluable, cuestionario a través del cual el propio usuario puede comprobar que conocimientos adquiridos tras escuchar un episodio del curso.

En este proyecto se ha utilizado un servidor web de la universidad Carlos III de Madrid, más concretamente del departamento de Seguridad Informática, para almacenar la información la web implementada.

4.2 Diseño de los episodios

En este apartado se va a explicar el diseño de los distintos apartados que forman el curso de criptografía.

En primer lugar se comenzó buscando información sobre los cursos de criptografía ya existentes. En primer lugar se buscó cualquier tipo de curso disponible en la web y luego se centró la búsqueda en cursos online de criptografía basados en podcasts. Después se comenzó a buscar información sobre el tema que se iba a tratar en el curso. Se obtuvo una gran cantidad de información que había que comenzar a clasificar y ordenar para poder comenzar a estructurar en diferentes episodios.

Tras definir los distintos episodios del curso, se comenzó su redacción dividiéndolos en apartados.

Todos los episodios del curso están divididos en apartados. Cada episodio tiene un primer apartado de introducción al tema que se va a tratar en él. A continuación se hablan de los tipos, ventajas e inconvenientes, aplicaciones y tipos. Finalmente cada episodio tiene un último apartado en el cual se resume el contenido que se ha tratado en el episodio.

Una vez redactados y corregidos todos los episodios, se procedió a traducirlos con la ayuda de un filólogo inglés para que la traducción realizada fuera correcta y adecuada.

Finalmente se grabaron los podcast, es importante recalcar que los podcast grabados en inglés los ha protagonizado una chica nativa, de esta manera se ha conseguido una mejor claridad y mayor entendimiento de estos en cuanto a la pronunciación de los mismos. Además para la introducción de cada podcasts se ha utilizado una música, es importante recalcar que esta música es gratuita y libre de derechos de autor.

4.3 Diseño de la interfaz

En este apartado se muestra el diseño de las interfaces de los dos prototipos distintos que tiene la web que se ha implementado para albergar el curso de criptografía online desarrollado. A continuación se mostrará el diseño de cada una de estas a través de una serie de figuras.

En primer lugar se va hablar de la página principal. Esta página sigue el mismo diseño que el resto de las páginas de la web implementada. Para la implementación de esta página se ha utilizado una plantilla libre y gratuita, ya que cumplía muchos de los requisitos de accesibilidad de la WCAG, como por ejemplo los colores entre otros. Estos requisitos son los que pide la ONCE para el desarrollo de páginas web orientadas a usuarios con alguna deficiencia visual. Además esta plantilla es sería y por eso aporta de una imagen de profesionalidad y seriedad a la web. Esto es importante porque se quiere mostrar la imagen de un curso serie y formal para que los usuarios confíen en él.

Esta página no tiene demasiados elementos, ya que es una página de introducción al curso, por lo que en ella se muestran objetivos principales que se pretenden conseguir con el desarrollo de este proyecto y la estructura en la que se divide el curso. Esta página es la única de la web que no contiene podcasts para reproducir, elementos descargables y autoevaluables.

A esta página se accede a través de la siguiente URL: www.seg.inf.uc3m.es/~lgmanzan/index.html .

En la Figuera 4.1 se puede ver una visión general de esta pantalla.

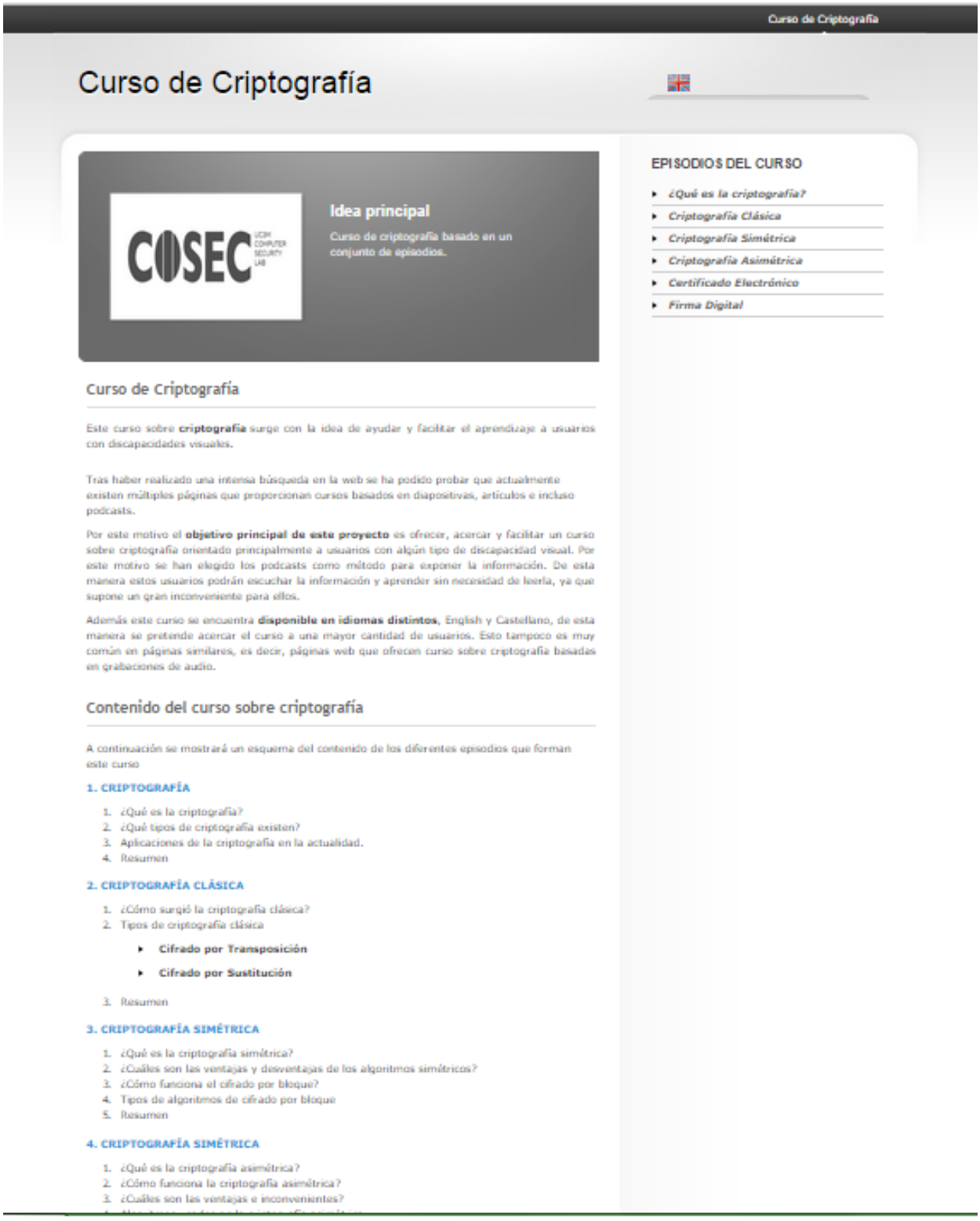

Figura 4.1 "Vista general de la página principal de la web"

Los diferentes elementos de esta pantalla se van a ir explicando y mostrando más detalladamente a continuación. Se van a ir explicando los diferentes elementos de esta página de arriba a abajo.

En primer lugar se puede encontrar el siguiente icono  en la página. Este icono sirve para cambiar el idioma de la página de castellano a inglés. Y de manera viceversa si el icono fuera una bandera de España.
Se decidió utilizar una imagen en vez de un botón con texto para ayudar más a los usuarios a reconocer el icono para el cambio de idioma, además de esta manera esta operación se puede realizar de una manera mucho más intuitiva.

Luego se pueden apreciar los enlaces a las distintas páginas de la web, es decir, estos son enlaces a las distintas páginas de la web. De esta manera existe navegabilidad entre las distintas páginas de la web, porque estos enlaces serán comunes para todas las páginas del sistema.
Estos enlaces se pueden apreciar en la figura 4.2.

Figura 4.2. “Enlaces a las distintas páginas de la web”

Además en el cuerpo de la web se puede apreciar un esquema de la estructura que tiene cada uno de los episodios del curso. En este esquema cada una de los títulos de los distintos episodios es un enlace hacía la página de cada uno de ellos.
También es importante recalcar que se ha utilizado un tamaño grande de letra para que los usuarios a los que principalmente va dirigido este curso online no encuentren demasiadas dificultades con el texto que tiene la página.

En la Figura 4.3 se puede ver una imagen de estos otros enlaces.

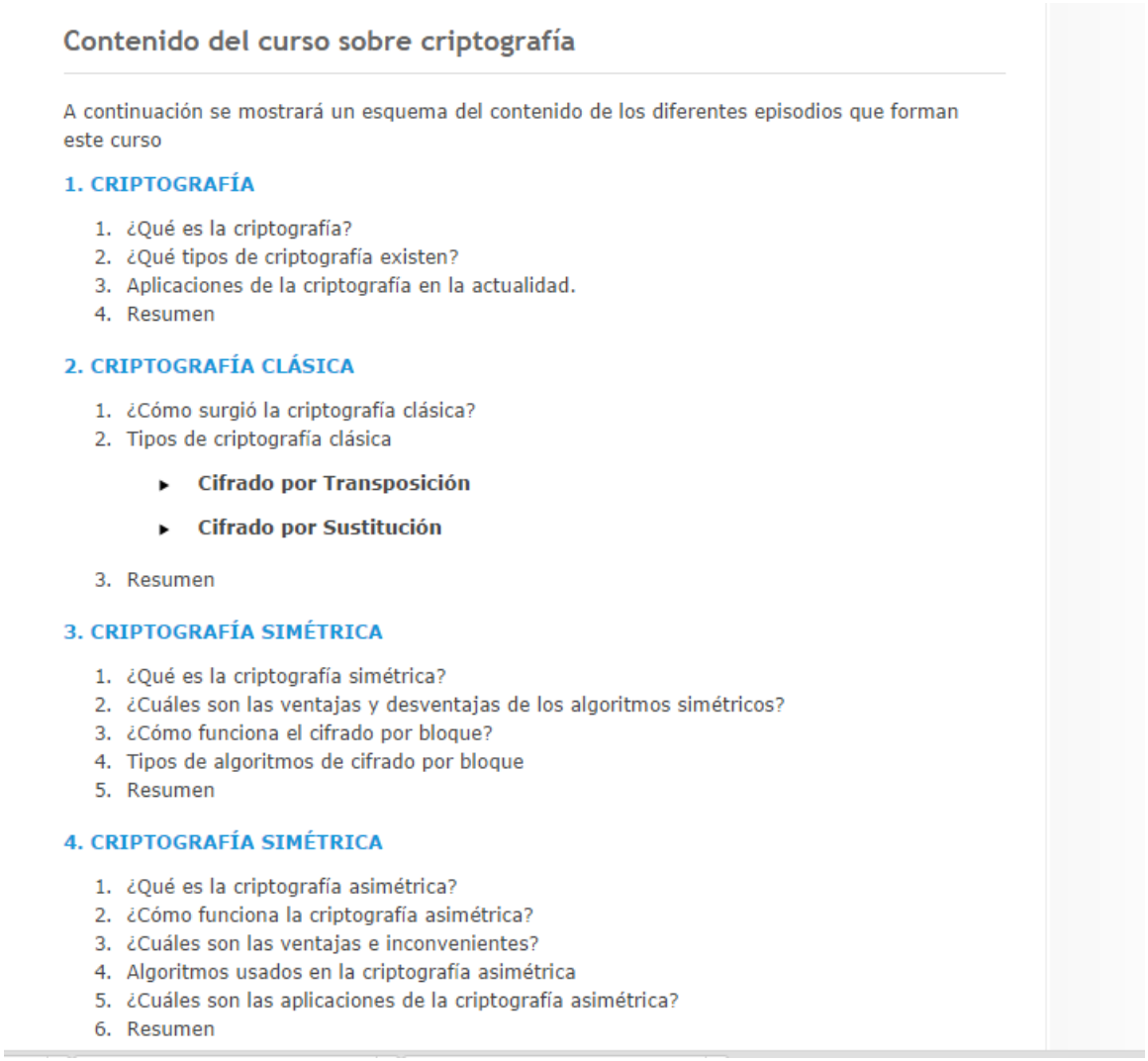

Figura 4.3. "Enlaces a los enlaces en la estructura del proyecto"

En segundo lugar se va a explicar el diseño del segundo tipo de páginas que se pueden encontrar en la web implementada para este proyecto o trabajo de fin de grado. Estas otras web son las específicas de cada episodio del curso. Cada episodio del curso tiene una web específica. En estas web se resumen los contenidos de los distintos episodios. Es importante recalcar que se ha utilizado un tamaño grande de letra para que los usuarios a los que principalmente va dirigido este curso online no encuentren demasiadas dificultades con el texto que tiene la página.

En la figura 4.4 se puede ver una imagen o visión global de una de estas páginas, esta concretamente se corresponde con el episodio 1 del curso.

Figura 4.5. Vista general de la página de un episodio"

Estas páginas tienen muchos más elementos que la página de inicio, a continuación se explicarán y mostrarán cada uno de ellos.

En primer lugar se puede encontrar el siguiente icono  en la página. Este icono sirve para cambiar el idioma de la página de castellano a inglés. Y de manera viceversa si el icono fuera una bandera de España.
Se decidió utilizar una imagen en vez de un botón con texto para ayudar más a los usuarios a reconocer el icono para el cambio de idioma, además de esta manera esta operación se puede realizar de una manera mucho más intuitiva.

Luego se pueden apreciar los enlaces a las distintas páginas de la web, es decir, estos son enlaces a las distintas páginas de la web. De esta manera existe navegabilidad entre las distintas páginas de la web, porque estos enlaces serán comunes para todas las páginas del sistema.
Estos enlaces se pueden apreciar en la figura 4.2.

Figura 4.2. "Enlaces a las distintas páginas de la web"

Ahora comienzan las diferencias principales con la página de inicio de la web.
Estas webs contienen una sencilla interfaz a través de la cual se puede reproducir, parar y reanudar audio. Además también se puede avanzar la reproducción de este y retrasarla o incluso modificar el audio.

La interfaz a través de la cual se pueden realizar toda esa serie de operaciones es la siguiente:

Figura 4.6. "Interfaz de reproducción de un podcast en reposo"

Figura 4.7. "Interfaz de reproducción de un podcast mientras se reproduce"

Después tenemos el botón de descargar un archivo de texto. En estos archivos de textos descargables se encuentra el contenido escrito de los podcast.
La imagen de este botón se puede apreciar en la figura 4.8.

Figura 4.8. "Vista del botón para descargar archivos de texto de la web"

Por último, los autoevaluables que sirven para que los propios usuarios puedan comprobar cuáles han sido los conocimientos adquiridos tras haber escuchado un episodio o podcast. Esto es algo que ninguno de los cursos sobre criptografía disponible actualmente en la web ofrece.

Las respuestas de estos formularios web no están ocultas, es decir, los usuarios según van contestando las distintas preguntas pueden ir viendo los resultados.
Se debe recalcar que el valor por defecto de una pregunta que no se ha contestado es "Incorrecta". La imagen de uno de estos evaluables se puede apreciar en la figura 4.9.

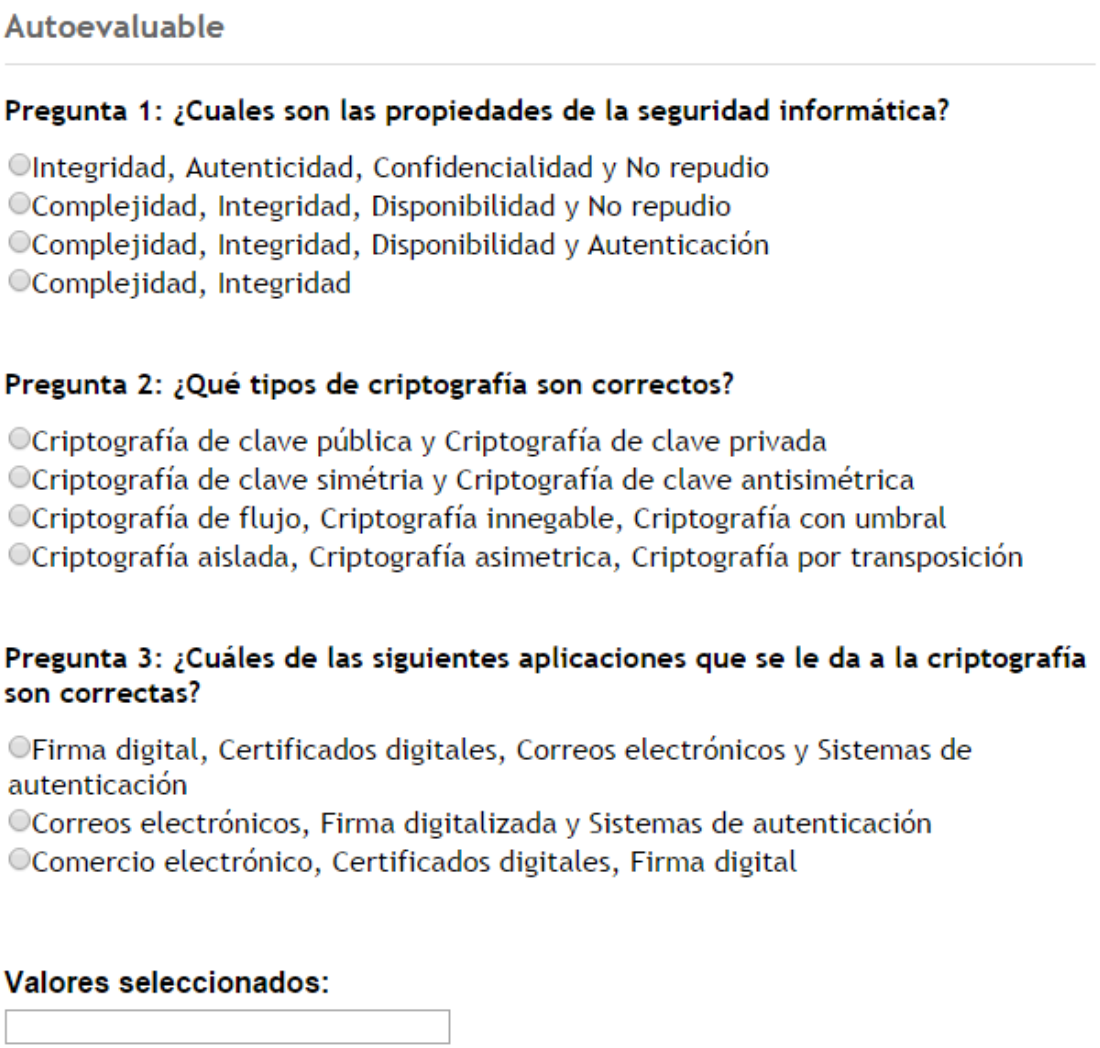

Figura 4.9. "Vista de un autoevaluable"

En la imagen 4.10 se puede ver como se muestran las respuestas cuando estas se han contestado en el autoevaluable.

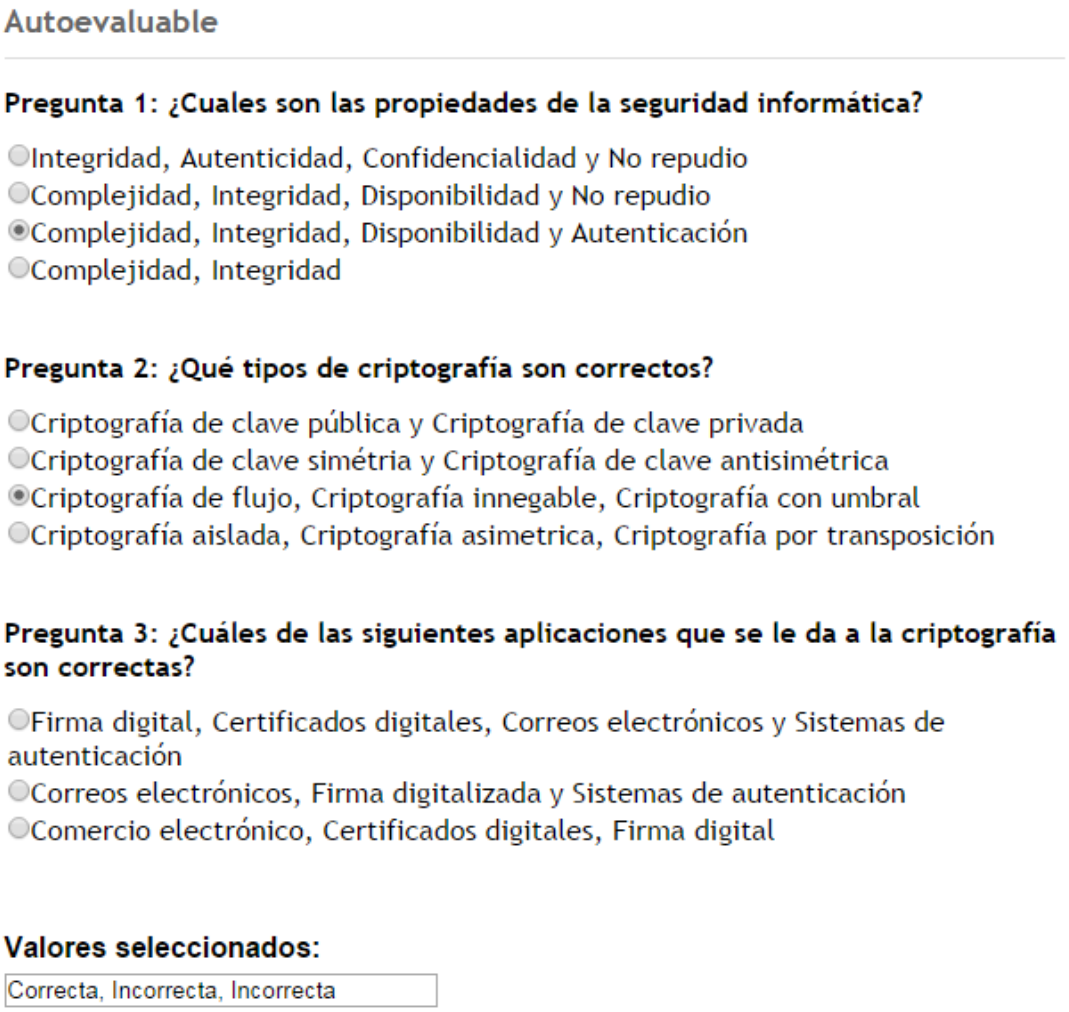

Figura 4.10. "Vista de un autoevaluable contestado"

Como se puede apreciar en la Figura 4.10 este autoevaluable ha sido contestado y en el cuadro de texto con título "Valores seleccionados" se muestran las respuesta. Se puede apreciar que en la pregunta 3 no se ha contestado nada y el valor que sale por defecto en las respuestas es "Incorrecta".

Capítulo 5

Gestión del proyecto

En este capítulo se van a detallar los aspectos referentes a la gestión del proyecto que incluyen la planificación del trabajo, los medios técnicos utilizados para el desarrollo de todo el proyecto así como el análisis económico del mismo.

5.1 Ciclo de vida del proyecto

El desarrollo de este proyecto se dividido en distintas etapas que han sido realizadas en un orden determinado. Estas etapas han sido definidas en el ciclo de vida del software. A través de la figura 5.1 se puede apreciar el modelo en cascada seguido en el desarrollo de este proyecto.

Figura 5.1. "Modelo en cascada elegido en este desarrollo"

La figura 5.1 muestra las distintas etapas que se han ido realizando de manera secuencial. En cada una de ellas se puede volver hacia detrás si en alguna de las fases anteriores se han producido errores o fallos o incluso se ha decidido realizar cambios.
Es importante que se explique que como este proyecto no es demasiado grande se ha elegido este modelo por ser un modelo sencillo.

5.2 Planificación

En este apartado se muestra la planificación inicial elaborada para el desarrollo del proyecto, en ella es posible apreciar las distintas fases en las que se ha descompuesto el proyecto como se ha explicado en el apartado anterior y además se pueden apreciar en la figura 5.1. Para el desarrollo de esta planificación se han tenido en cuenta jornadas de trabajo diarias de 4 horas en días laborables. La causa de esta planificación se debe a que se ha tenido que compaginar el desarrollo de este proyecto con la realización de un trabajo a jornada completa y la realización de dos asignaturas.

La planificación inicial del proyecto comienza el día 2 de julio y termina el 18 de septiembre. Este tiempo comprende 57 días laborales, es decir, 228 horas. Esto se puede apreciar en el diagrama de Gantt mostrado en la Figura 5.2.

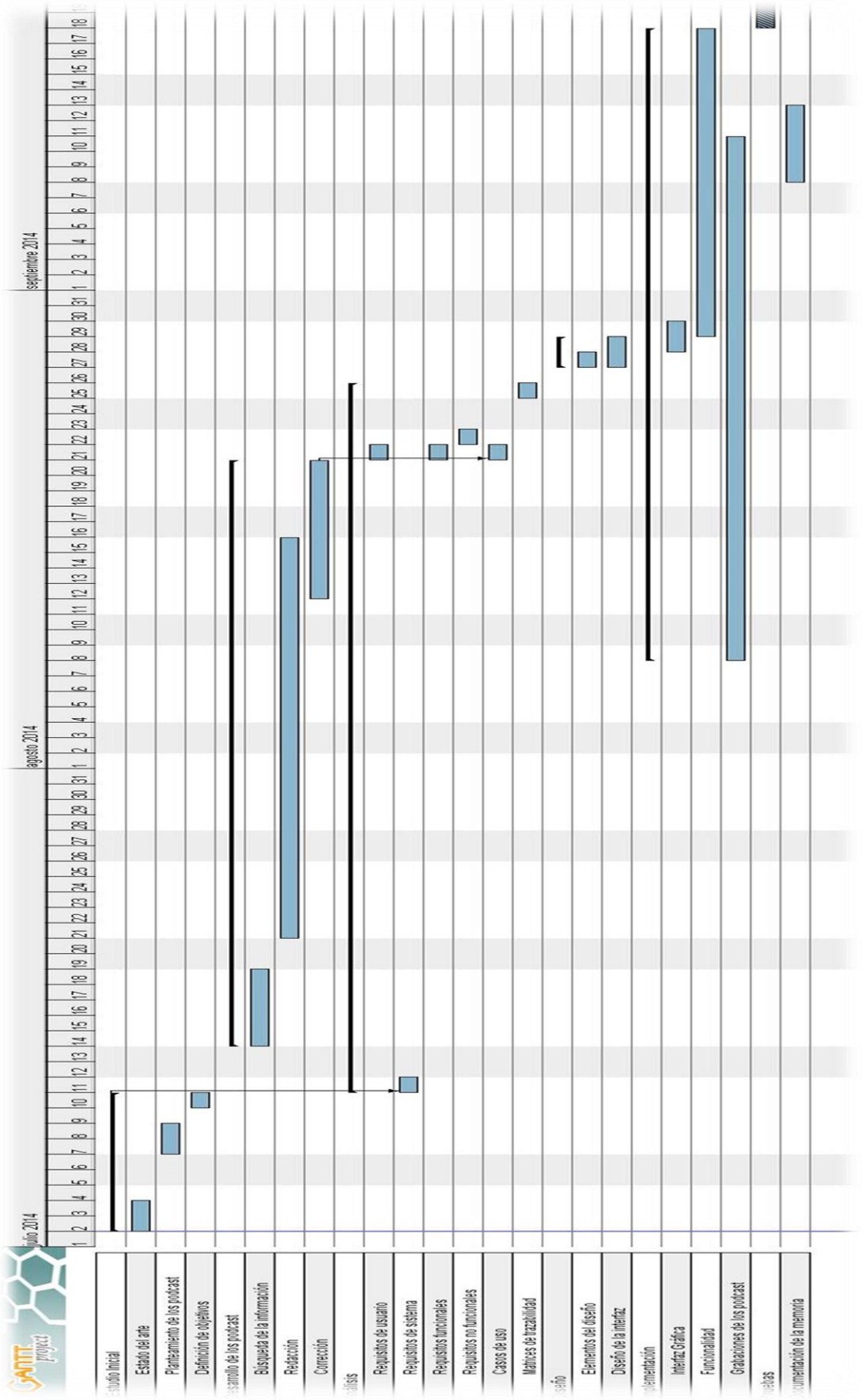

Figura 5.2. "Diagrama de Gantt"

Tabla 5.1. "Visión inicial detallada del proyecto"

Trabajo fin de grado	**57 días**	**02 /07/2014**	**18/09/2014**
Estudio del arte	2 días	2/07/2014	4/07/2014
Planteamiento de los podcasts	2 días	7/07/2014	9/07/2014
Definición de los objetivos	1 días	10/07/2014	11/07/2014
Búsqueda de la información	5 días	14/07/2014	19/07/2014
Redacción de los podcasts	20 días	21/07/2014	16/08/2014
Corrección de los podcasts	7 días	12/08/2014	21/08/2014
Requisitos funcionales	1 días	21/07/2014	22/08/2014
Requisitos no funcionales	1 días	22/08/2014	23/08/2014
Casos de uso	1 días	21/08/2014	22/08/2014
Matrices de trazabilidad	1 días	25/08/2014	26/08/2014
Elementos del diseño	1 días	27/08/2014	28/08/2014
Diseño de la interfaz	2 días	27/08/2014	29/08/2014
Implementación de la interfaz gráfica	2 días	28/08/2014	30/08/2014
Implementación de la funcionalidad	14 días	29/08/2014	18/09/2014
Grabación de los podcasts	24 días	8/08/2014	11/09/2014
Pruebas	2 días	18/09/2014	20/09/2014
Documentación de la memoria	5 días	8/09/2014	13/09/2014

Como se puede apreciar en la figura 5.2 y en la tabla 5.1 la mayor parte del tiempo estimado para el desarrollo de este proyecto está reservado al diseño y desarrollo de los podcasts.

5.3 Desarrollo real del proyecto

En este apartado se muestra el tiempo real que ha sido destinada para la realización del proyecto y además esta se compara con la planificación inicial para ver y estudiar las desviaciones que han ido surgiendo a lo largo del desarrollo.

En la tabla 5.2 se muestra el desarrollo final del proyecto. En esta tabla se puede apreciar que el reparto de tiempos es parecido al realizado inicialmente, pero la duración de alguna tarea ha necesitado un tiempo mayor al planificado. Esto se puede observar con mayor detalle en la tabla 5.2 que muestra el desarrollo real detallado de este proyecto.
En dicha tabla se puede apreciar que la duración real del proyecto ha sido de 67 días (se ha incluido un fin de semana) frente a los 57 planificados inicialmente, es decir, se ha tardado 268 horas en realizar este proyecto, mientras que inicialmente se planificaron 228 horas.

Se finalizó el proyecto el 23/09/2014 ya que la documentación de este tuyo un retraso. Además no se contempló en la planificación inicial la corrección de esta y eso ha sido el detonante de que el proyecto finalizará ese día.

Tabla 5.2. "Tiempo real empleado en la realización del proyecto"

Trabajo fin de grado	**67 días**	**02 /07/2014**	**23/09/2014**
Estudio del arte	2 días	2/07/2014	4/07/2014
Planteamiento de los podcasts	2 días	7/07/2014	9/07/2014
Definición de los objetivos	1 días	10/07/2014	11/07/2014
Búsqueda de la información	6 días	14/07/2014	20/07/2014
Redacción de los podcasts	23 días	21/07/2014	31/08/2014
Corrección de los podcasts	7 días	12/08/2014	21/08/2014
Requisitos funcionales	1 días	21/07/2014	22/08/2014
Requisitos no funcionales	1 días	22/08/2014	23/08/2014
Casos de uso	1 días	21/08/2014	22/08/2014
Matrices de trazabilidad	1 días	25/08/2014	26/08/2014
Elementos del diseño	1 días	27/08/2014	28/08/2014

Diseño de la interfaz	2días	27/08/2014	29/08/2014
Implementación de la interfaz gráfica	2 días	28/08/2014	30/08/2014
Implementación de la funcionalidad	14 días	29/08/2014	18/09/2014
Grabación de los podcasts	27 días	8/08/2014	14/09/2014
Pruebas	2 días	18/09/2014	20/09/2014
Documentación de la memoria	8/09/2014	8/09/2014	14/09/2014

A continuación en la tabla 5.3 se puede valorar la desviación que ha sufrido el proyecto de una manera más precisa ya que se coteja con la planificación inicial con la real. En esta tabla se puede observar que la planificación inicial ha sufrido una desviación del 17,54 %. Esta desviación viene derivada por las distintas dificultades que se han ido encontrando durante la realización de las tareas. Además también se pueden encontrar desviaciones causadas por haber realizado una sobreestimación en algunas tareas de la planificación inicial. Estos motivos junto con las variaciones en la disponibilidad, como se explicó anteriormente han llevado al proyecto a tener una pequeña desviación del 17,54%.

Tabla 5.3. "Análisis de desviación en la planificación"

Trabajo fin de grado	Planificado	Real	Diferencia	Variación
Planificación inicial	**57 días**	**67 días**	**10 días**	**17.54%**
Estudio del arte	2 días	2 días	0 días	0%
Planteamiento de los podcasts	2 días	2 días	0 días	0%
Definición de los objetivos	1 días	1 días	0 días	0%
Búsqueda de la información	5 días	6 días	1 días	20%
Redacción de los podcasts	20 días	23 días	5 días	25%
Corrección de los podcasts	7 días	7 días	0 días	0%
Requisitos funcionales	1 días	1 días	0 días	0%
Requisitos no funcionales	1 días	1 días	0 días	0%
Casos de uso	1 días	1 días	0 días	0%

Matrices de trazabilidad	1 días	1 días	0 días	0%
Elementos del diseño	1 días	1 días	0 días	0%
Diseño de la interfaz	2 días	2días	0 días	0 %
Implementación de la interfaz gráfica	2 días	2 días	0 días	0%
Implementación de la funcionalidad	14 días	14 días	0 días	0%
Grabación de los podcasts	24 días	27 días	3 días	12.5%
Pruebas	2 días	2 días	0 días	0%
Documentación de la memoria	5 días	7 días	1 días	20%

Capítulo 6

Presupuesto

En este capítulo de va a realizar un pequeño análisis económico del proyecto. En el cual se habla del presupuesto inicial del proyecto, el presupuesto para el cliente y el coste real del proyecto. Para el desarrollo de esta sección se ha seguido plantilla proporcionada en la web de la universidad [22].

6.1 Presupuesto Inicial

El este apartado se muestra el presupuesto inicial donde se van a especificar los costes que han sido presupuestados para todo el proyecto junto con el presupuesto total estimado.
El necesario especificar que el 21% de IVA no está incluido en ninguno de los gastos expuestos en este capítulo.

6.1.1 Gastos de personal

En la tabla 6.1 se especifica los gastos de personal. Para realizar este cálculo se ha tenido en cuenta la dedicación de un ingeniero para el desarrollo de este proyecto. Teniendo en cuenta que dicho ingeniero ha dedicado 4 horas al día durante 62 días, es decir, un total de 248 horas.

El coste de un Ingeniero por hora se ha tomado de las tarifas que tiene actualmente Accenture. En las tarifas de dicha empresa el coste de un ingeniero por hora son 45€.
Para realizar los cálculos de la tabla 6.1 se han tomado 22 días laborables / mes y tomando los datos que ponen en la página de la seguridad social se ha tomado un 28.3% como el porcentaje a pagar para el régimen general de la Seguridad Social.

Tabla 6.1. "Tabla de coste de materiales"

Trabajador	Horas dedicadas	Coste trabajador / mes	Coste Bruto	Seguridad Social	Total
Ingeniero	252 horas	3.960 €/ mes	11.340€	3.209,22€	14.549,22 €

El coste total de Personal para la realización de este proyecto según un ingeniero de la empresa Accenture es de 14.549,22 €.

6.1.2 Gastos de equipos

En este apartado se van a especifican los gastos relacionados con los equipos utilizados en el desarrollo de este proyecto. Estos equipos son un ordenador portátil, un teléfono móvil, una Tablet y unos auriculares con micrófono. En la tabla 5.2 se van a especificar de una manera más detallada los costes imputables para cada equipo o recurso empleado.

Los periodos de depresiones que se ha tomado para el ordenador es el usado en el ámbito de la administración general. Por otro lado los periodos de depresión usados en el móvil, auriculares y Tablet son los periodos de lanzamientos entre los nuevos modelos.

Tabla 6.1. "Tabla de gastos de equipos"

Equipos	Coste	Dedicación	Dedicación	Coste imputable
Portátil Asus K551 LN-XX 182 H	899€	2.93 meses	36 meses	73.17 €
Móvil: Samsung Galaxy S3 de 32GB	450 €	2.93 meses	24 meses	54.94 €
Auriculares con micrófono	50 €	2.93 meses	24 meses	6.10 €
Tablet: Aipad pantalla retina	379€	2.93 meses	24 meses	46.27 €
Total imputable	180.48 €			

Es importante recalcar que el coste es el precio de venta al público sin IVA.

6.1.3 Gastos software

En este apartado se han detallado los gastos software que se han tenido en el desarrollo de este proyecto. En la tabla 6.2 se pueden apreciar estos gastos de una manera más detallada.

Tabla 6.2. "Tabla de los gastos software"

Equipos	Coste	Dedicación	Dedicación	Coste imputable
Microsoft Office 2011	116.81€	2.93 meses	36 meses	2.44 €
Total imputable	2.44 €			

Es importante recalcar que el coste es el precio de venta al público sin IVA.

6.1.4 Gastos de consumibles

En este apartado se detallan los gastos que se han tenido en concepto de consumibles. En este caso dichos gastos se relacionan con el material de oficina, folios, bolígrafos, etc, que se han utilizado en la realización de este proyecto.

En la tabla 6.3 se pueden ver estos costes de manera más detallada.

Tabla 6.3. "Tabla de gastos de consumibles"

Gastos	Coste Unitario	Cantidad	Coste Total
Material de oficina	20 €	1	20 €

Es importante recalcar que el coste unitario es el precio de venta al público sin IVA.

6.1.5 Estimación de costes

En este último apartado se muestra la estimación completa de gastos realizada a lo largo de este capítulo. En la tabla 6.4 se puede apreciar de una manera más detallada esta estimación de costes.

Tabla 6.4. "Tabla de gastos totales"

Gastos	Coste
Gastos de personal	14.318,28 €
Gastos de equipos	180.48 €
Gastos software	2.44 €
Gastos de consumibles	20 €
Total	14.521,2 €

Es importante recalcar que el coste es el precio de venta al público sin IVA.

Capítulo 7

Conclusiones

7.1 Conclusiones

Como se dijo en el primer capítulo de este documento uno de los principales objetivos de este proyecto es ofrecer, acercar y facilitar un curso sobre criptografía orientado principalmente a usuarios con algún tipo de deficiencia visual. Por este motivo se han eligió los podcasts como formato para exponer la información. De esta manera estos usuarios pueden escuchar y aprender sin necesidad de leer la información.

El segundo objetivo principal de este curso era llegar al mayor público posible. Por este motivo la utilización de los podcasts favoreció este hecho. La información escuchada es más atractiva, amena y divertida para el resto de usuarios del curso, a pesar de que los usuarios principales tienen alguna deficiencia visual. Además la web se ha desarrollado en dos idiomas, también los podcasts, con el fin de poder llegar a un mayor número de usuarios.

El último objetivo de este curso era que todos los usuarios aprendieran que es la criptografía, su historia, los diferentes tipos que hay y las distintas aplicaciones que se le da actualmente. Para conseguir este objetivo se han implementado unos autoevaluable

para que los usuarios puedan comprobar y mediar los conocimientos que han adquirido tras haber realizado cualquiera de los episodios del curso.

Tras haber realizado este proyecto se puede comprobar que todos y cada uno de los objetivos principales que se definieron en el capítulo 1 de este documento se han conseguido.

Por este motive se puede concluir con que este curso a dado los resultados que se esperaban, por lo que podría ser utilizado como método de aprendizaje para alumnos con algún tipo de deficiencia visual.

7.2 Dificultades del proyecto

A continuación se expondrán las principales dificultades encontradas en el desarrollo de este proyecto.

En primer lugar se encontró la dificultad de diseñar un podcast. En este tipo de archivos la información debe explicarse de una manera diferente, insistiendo o incidiendo en varias ocasiones en los puntos más importantes, ya que el usuario debe recordarlos.

Otro problema que se ha encontrado en el desarrollo de este proyecto es la grabación de los podcasts, ya que se debe leer la información dando una entonación determinada, realizando las pausas de los símbolos de puntuación y vocalizando muy bien mientras se habla o lee. Además los que se han grabado en inglés ha requerido el uso de una persona nativa, para que el podcast se entendiera sin ningún problema.

El último problema encontrado en el desarrollo de este proyecto se ha dado en la etapa de implementación de la web. Cada uno de los episodios de este proyecto tiene un autoevaluable en el cual el usuario puede comprobar lo aprendido en el podcast escuchado anteriormente. Estos autoevaluables se diseñaron con las respuestas ocultas, de esta manera los usuarios debían seleccionar una opción para poder ver las respuestas correctas del formulario.
La implementación de esta opción de las respuestas ocultas utilizando en el formulario web radio button dio muchos problemas, ya que resulta prácticamente imposible chequear si un radio button se ha seleccionado o no.
Finalmente para solucionar este problema se buscó una alternativa que en la cual las respuestas no están ocultas pero se muestran de una manera diferente a las habituales actualmente.

Capítulo 8

Trabajos futuros

La principal aplicación de este tipo de cursos en el futuro sería la docencia, ya que resultaría muy beneficioso para los usuarios. Actualmente el material de apoyo proporcionado en las distintas asignaturas de una carrera, etc., están basados en artículos, libros, diapositivas, etc. Este tipo de material de apoyo suele ser muy aburrido, denso e incluso a veces difícil de comprender por el tipo de lenguaje que utiliza, o por la lengua en el cual está escrito.

Con la implantación de este tipo de cursos en la docencia se podrían resolver y evitar estos problemas, ya que los podcasts resultan mucho más a menos, divertidos y fáciles de entender. Podrían ser utilizados por cualquier usuario independientemente del país de procedencia, las deficiencias visuales que tenga, etc.

Además de esta manera cualquier usuario con algún tipo de deficiencia visual podría utilizar el mismo material de apoyo que el resto de alumnos de su misma clase, sin que la utilización de está suponga un reto para ellos.

Pero centrándonos un poco en el curso desarrollado, en próximos trabajos se podría ampliar o incluso realizar varios cursos sobre temas relacionados con la seguridad informática que tengan relevancia para los usuarios en la actualidad. De esta manera se tendría un curso sobre seguridad informática basado en subcursos.

De esta manera cualquier usuario podría aprender conceptos básicos y el funcionamiento de temas relevantes en la actualidad, cumpliéndose uno de los objetivos principales de este proyecto, el que este curso pueda llegar al mayor número posible de usuarios.

Glosario

FTP	*File Transfer Protocol*
FTPS	*File Transfer Protocol/Secure Sockets Layer*
HTML	*Hyper Text Markup Language*
HTTP	*Hypertext Transfer Protocol*
IVA	*Impuesto sobre el Valor Añadido*
LPI	*Laboratorio de Procesado de Imagen*
ONCE	*Organización Nacional de Ciegos Españoles*
PDF	*Portable Document Format*
PERT	*Project Evaluation and Review Techniques*
RAE	*Real Academia Española*
SFTP	*SSH File Transfer Protocol*
SSH	*Secure SHell*
URL	*Uniform Resource Locator*
WAI	*Web Accesibility Initiative*
WCAG	*Web Content Accessibility Guidelines*
WWW	*World Wide Web*
W3C	*World Wide Web Consortium*

Referencias

[1] Microsoft Office. Disponible [Internet]: <http://office.microsoft.com/>
[2 de Septiembre de 2014]

[2] Audacity 2.0.5. Disponible [Internet]: <http://audacity.sourceforge.net/?lang=es>
[24 de septiembre de 2014]

[3] Notepad ++. Disponible [Internet]: <http://notepad-plus-plus.org/>
[24 de septiembre de 2014]

[4] JavaHispano Podcast Disponible [Internet]: <http://www.javahispano.org/podcast/>
[24 de septiembre de 2014]

[5] Crimen Digital. Disponible [Internet]: <http://www.crimendigital.com/>
[24 de septiembre de 2014]

[6] Ivoox - audioKiosko. Disponible [Internet]:
<http://www.ivoox.com/audios_sa_f_1.html>
[24 de septiembre de 2014]

[7] TheadPost. Disponible [Internet]: < http://threatpost.com/category/cryptography>
[24 de septiembre de 2014]

[8] Más adelante. Disponible [Internet]: <http://www.masadelante.com/faqs/podcast>
[10 de septiembre de 2014]

[9] Definición de. Disponible [Internet]: <http://definicion.de/ />
[5 de septiembre de 2014]

[10] GanttProject. Disponible [Internet]: <http://www.ganttproject.biz/>
[1 de Septiembre de 2014]

[11] Pergamino virutal. Disponible [Internet]: < http://www.pergaminovirtual.com.ar/>
[4 de Septiembre de 2014]

[12] Mini curso de criptografía. Disponible [Internet]:
<http://www.cyberhades.com/2011/01/10/criptografia-teoria-y-practica-mini-curso/>
[10 de enero de 2011]

[13] Curso básico de criptografía. Disponible [Internet]:
<http://www.kriptopolis.com/criptografia-clasica-i>
[2 de junio de 2012]

[14] Programas Internacionales de Cooperación Tecnológica. Disponible [Internet]:
<https://www.cdti.es/index.asp?MP=7&MS=563&MN=3&IDR=77>
[25 de agosto de 2013]

[15] RA. Disponible [Internet]: <http://www.rae.es/>
[14 de junio de 2011]

[16] LPI. Disponible [Internet]:
http://www.lpi.tel.uva.es/~nacho/docencia/ing_ond_1/trabajos_01_02/estudios_de_grabacion/introduccion.html
[4 de junio de 2014]

[17] Universidad Pompeu Fabra. Disponible [Internet]: <http://www.upf.edu/es/>
[8 de agosto de 2014]

[18] Seguridad de la Información. Disponible [Internet]:
<http://www.segu-info.com.ar/criptologia/criptologia.html>
[21 de septiembre de 2014]

[19] Consultoría PyME. Disponible [Internet]:
<http://www.consultoria-pyme.com/108-1-%BFQue+es+un+Podcast%3F.html>
[20 de septiembre de 2014]

[20] Yuml. Disponible [Internet]: < http://yuml.me/>
[19 de septiembre de 2014]

[21] Coffee Cup. Disponible [Internet]: <http://www.coffeecup.com/free-ftp/>
[19 de septiembre de 2014]

[22] Universidad Carlos III de Madrid [Internet]: www.uc3m.es/Inicio
[22 de septiembre de 2014]